

UNITED STATES DISTRICT COURT

for the
Southern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

See Attached Affidavit and its Attachment A

20 MAG 00669

Case No.

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attached Affidavit and its Attachment A

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)

Offense Description(s)

18 U.S.C. §§ 2252A(a)(2) distribution, receipt, and possession of child pornography
and (a)(5)

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Thomas A. Thompson, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/17/2020

City and state: New York, NY

Judge's signature

Hon. Katharine H. Parker, USMJ

Printed name and title

USAO_000004

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

20 MAG 00669

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for the Premises Known and Described as 221 Husson Avenue, Bronx, New York 10473 and Any Closed Containers/Items Contained Therein, USAO Reference No. 2020R00064

SOUTHERN DISTRICT OF NEW YORK, ss.:

THOMAS A. THOMPSON, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation (the "FBI") and am one of the law enforcement officers with primary responsibility for the instant investigation. I have been employed by the FBI for 15 years. During that time, I have participated in numerous investigations of child exploitation crimes, including crimes involving child enticement and child pornography. I have participated in the execution of numerous search warrants involving electronic evidence. I have received training in the areas of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (the "Subject Premises") for, and to seize, the items and information described in Attachment A. This affidavit

2017.08.02

USAO_000005

is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESP”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The Subject Premises are particularly described as 221 Husson Avenue, Bronx, New York 10473. The Subject Premises is a two-story residence with white and green siding. A metal fence is in front of the residence. There is a mailbox in front of the residence with the numbers “221,” in gold numbering, on the front of the mailbox. There are two entrances to the Subject Premises, one on each floor. The first-floor entrance to the Subject Premises is on the left side of the front of the residence. The second-floor entrance to the Subject Premises is on the right side of the front of the residence. To the right of the second-floor entrance are the numbers “221” in black numbering. Below is a photograph of the Subject Premises:



C. The Subject Offenses

4. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Premises contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) and (a)(5), that is, distribution, receipt, and possession of child pornography (the “Subject Offenses”).

II. Background of the Investigation and Probable Cause

5. The instant investigation involves a user of “Freenet” — which is an Internet-based, peer-to-peer (P2P) network that allows users to anonymously share files, chat on message boards, and access websites within the network. Law enforcement agents have been investigating child pornography trafficking by Freenet users since at least 2011.

A. Background Regarding Freenet

6. In order to access Freenet, a user must first download the Freenet software, which is free and publicly available. The Freenet “source code” — i.e., the computer programming code that facilitates Freenet’s operation — is also publicly available. In other words, Freenet is “open

source” software that may be examined and analyzed by anyone with the pertinent expertise or knowledge.

7. Anyone running the Freenet software may join and access the Freenet network. Each computer running Freenet connects directly to other computers running Freenet, which are called its “peers.”¹ When installing Freenet, each user agrees to provide to the network a portion of the storage space on the user’s computer hard drive, so that files uploaded by Freenet users can be distributed and stored across the network. Freenet users can upload files into the Freenet network and download files from the Freenet network. After a user installs Freenet on the user’s computer, the software creates a default “download” folder. If a user successfully downloads a particular file from Freenet, Freenet may save the content of that file to the “download” folder. A user may change this default setting and direct the content to be downloaded elsewhere.

8. When a user uploads a file into Freenet, the software breaks the file into pieces (called “blocks”) and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Freenet network of peers.² The software also creates an index that contains a list of all of the pieces of the file and a unique key – a series of letters, numbers and special characters – that is used to download the file.³

9. In order to download a file on Freenet, a user must have the key for the file. There are a number of ways that a Freenet user can download a file using a key. Some examples include: (1) the “download” box on Freenet’s “file sharing” page; (2) the “download” box on the message

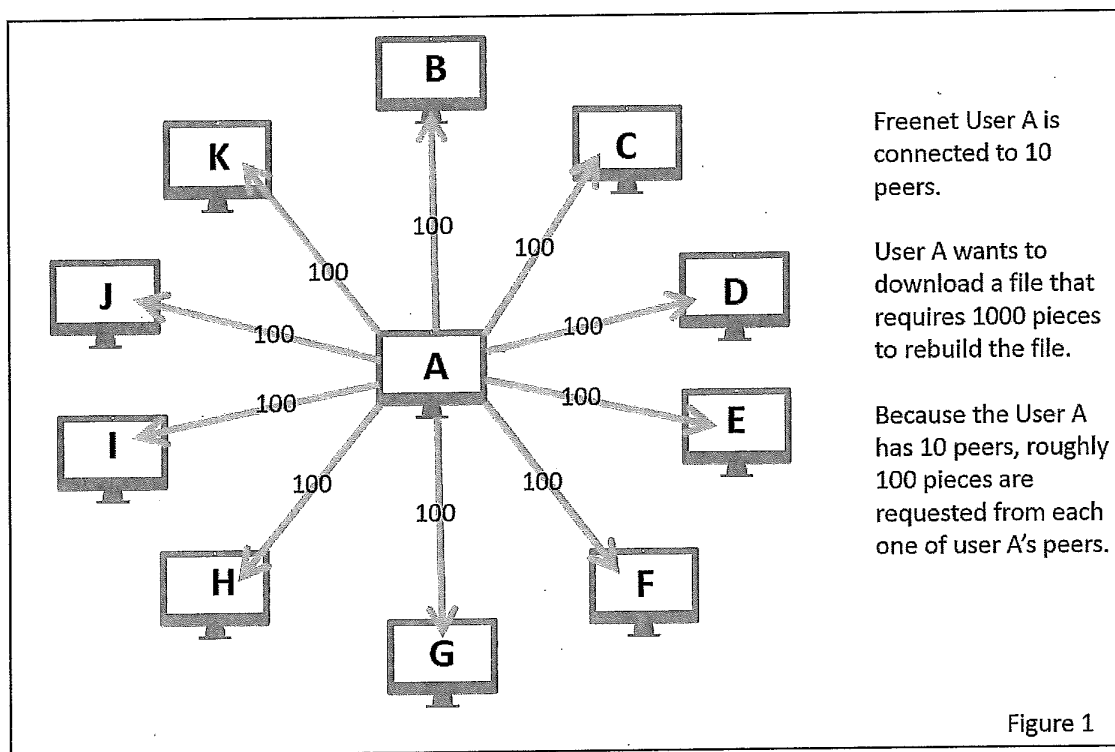
¹ The number of peers is determined by the user’s settings and is based on the quality and speed of the user’s Internet connection.

² Because the pieces of files are encrypted, a Freenet user is unable to access the content of pieces that are stored on the user’s computer hard drive, which are not in a readable format.

³ An example key is: CHK@0R6h6o8a~JbOGg8GmxGauRyqJPSwcHGmxGauLznw8FeyB0go,08agxRpNx~wc~rmZRfWQaSed3HTeKKkXAwvDRF2LUaU,AAMC--8/lolitz49.avi.

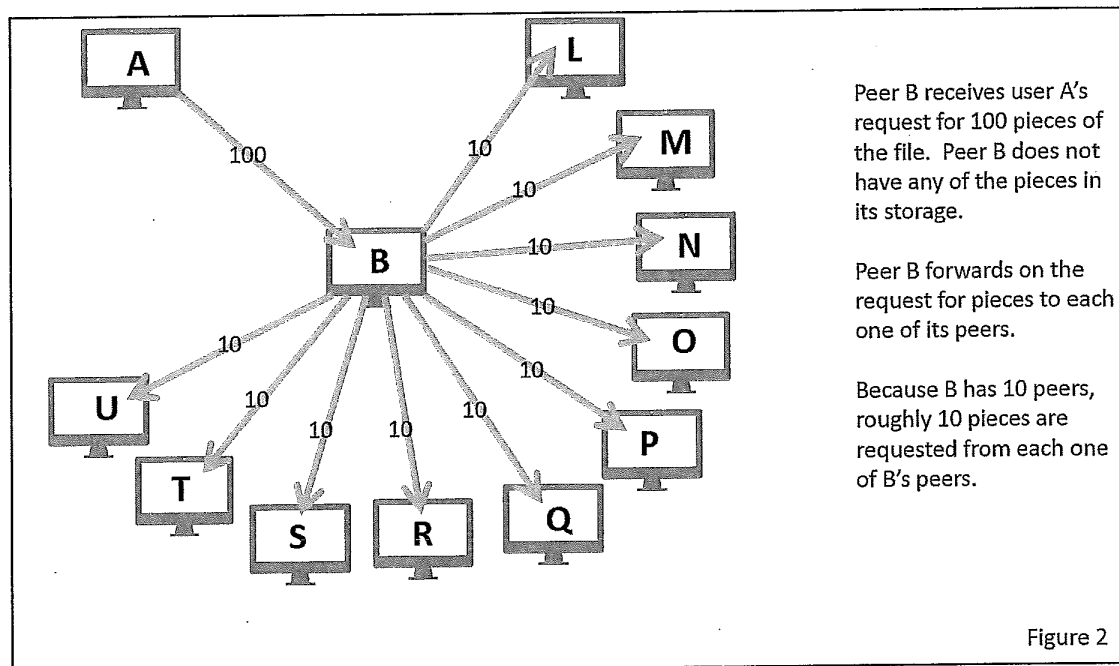
board associated with Freenet or other Freenet add-on programs; and (3) directly through the user's web browser while the user is connected to the Freenet network.

10. When a user attempts to download a file via Freenet, Freenet downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The Freenet software then requests all of the pieces of the file from the user's peers. Rather than request all of the file pieces from a single peer, requests for file pieces are divided up in roughly equal amounts among the user's peers. If a user's peer does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on. For example, if User "A" has 10 peers and requests 1000 pieces of a file, roughly 100 pieces are requested from each one of User A's peers. See Figure 1.



If Peer "B" receives User A's request for 100 pieces of the file, but does not have any of those pieces in its storage, Peer B forwards on the request for those pieces to Peer B's peers. If Peer B

has 10 peers of its own, roughly 10 pieces are requested from each one of Peer B's peers. See Figure 2.



As noted below, this design can help law enforcement distinguish between a Freenet user that is the original requestor of a file, and one that is merely forwarding the request of another user.

11. To prevent requests for pieces from going on indefinitely, Freenet is configured to only allow a request for a piece of a file to be forwarded to another peer a limited number of times (the default maximum is 18). If a request reaches that limit without finding the requested piece, a signal is returned to the user's computer and the request is sent to another of the user's peers. The remaining number of times a request for a piece may be forwarded is included within the request for that piece.

12. Freenet attempts to hide which computer uploaded a file into or downloaded a file from the network by making it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer (i.e., the peer was the "original requestor" of the file), or

whether that peer was simply forwarding a different peer's request. Freenet attempts to hide the identity of the original requestor by randomizing the initial number of times a request can be forwarded from one peer to another to be either 17 or 18. Without this randomization, any time a user received a request for a piece of a file that could be forwarded 18 times, the user would know that its peer was the original requestor of the file. This design allows investigators using Freenet to focus investigative efforts on peer computers that request pieces of files of interest that may be forwarded 17 or 18 times, in order to determine whether the peer was the original requestor of the file.

13. Freenet has two operational modes, "Darknet" and "Opennet." In the Darknet mode, a computer connects only to peers whom the user has specifically selected. In the Opennet mode, a computer may connect to peers unknown to the user. A Freenet user may choose which mode to use. The mode relevant to this investigation involves a user who chose to use the Opennet operational mode.

14. Freenet warns its users in multiple ways that it does not guarantee anonymity: when Freenet software is initially installed; within the log file each time Freenet is started; and via Freenet's publicly accessible website. Freenet software also does not mask a computer's IP address — the IP addresses of each Freenet user's peers are observable to the user. For example, if a user is connected to 10 peers on Freenet, all 10 of those peers' IP addresses will be observable to the user. The fact that Freenet does not mask IP addresses is explained on its publicly accessible website. Freenet also acknowledges on its publicly accessible website that, for users who use the Opennet mode, it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers.

B. Child Pornography Images/Videos on “Freenet”

15. Freenet can be used to advertise and distribute images and videos of child pornography. Unlike other file sharing systems, Freenet does not provide a search function for its users whereby users would insert search terms to locate files. Therefore, a user who wishes to locate and download child pornography from Freenet must identify the key associated with a particular child pornography file and then use that key to download the file.

16. Freenet users can identify those keys in a number of ways. For example, “message boards” exist on Freenet that allow users to post textual messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled: “pthc,” “boy porn,” “hussy,” “pedomom,” “kidfetish,” “toddler_cp,” “hurtcore,” and “tor-childporn.” Typical posts to those message boards contain text, keys of child pornography files that can be downloaded through Freenet, and in some cases descriptions of the image or video file associated with those keys.

17. Freenet users can also obtain keys of child pornography images or videos from websites that operate within Freenet called “Freesites.” Freesites can only be accessed through Freenet. Some of those sites contain images of child pornography the user can view along with keys of child pornography files. It is also possible that Freenet users may obtain keys related to child pornography images or videos directly from other Freenet users.

C. Investigation into Trafficking of Child Pornography on Freenet

18. Since approximately 2011, law enforcement has been investigating the trafficking of child pornography on Freenet. A modified version of the Freenet software is available to sworn law enforcement officers to assist in conducting Freenet investigations. I have been trained on the

operation of the modified law enforcement version of Freenet. This law enforcement version is nearly identical to Freenet, except that it allows a computer operated by a law enforcement officer to automatically log information about requests for pieces of files received directly from its peers. The types of information logged by a law enforcement computer are available to all standard Freenet users as part of Freenet's normal operation. This information includes, but is not limited to: the IP addresses of the user's peers; the number of peers those peers report to have; a unique identifier assigned by the software (referred to as the computer's Freenet "location"); the remaining number of times a request for a piece of a file may be forwarded; the date/time of requests received from a peer; and the digital hash value of a requested piece.

19. Law enforcement computers do not target specific peers on Freenet nor do law enforcement computers solicit requests from any peers. The Freenet information collected by law enforcement computers is logged and provided to other Freenet-trained law enforcement personnel in order to further investigations into Freenet users believed to be downloading child pornography files through Freenet.

20. Law enforcement officers collect keys associated with suspected child pornography files that are being publicly shared and advertised on Freenet. Law enforcement only investigates Freenet users who request pieces of files associated with such keys collected by law enforcement. The keys collected by law enforcement have been obtained via publicly accessible sites, such as Freenet message boards and Freesites, as well as during the course of prior investigations into child pornography trafficking on Freenet. This investigation pertains to child pornography files with known keys, the content of which are further described below. Those files are referenced as "files of interest."

21. By viewing the documented activity of a peer that sends a request to a law

enforcement computer, it is possible to determine whether it is significantly more probable than not that the peer is the original requestor of a file of interest. Only those requests that were intended for law enforcement computers as recipients, that may be forwarded 17 or 18 times, and are associated with a file of interest are analyzed. A mathematical formula is then applied to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer.

22. I have reviewed a peer-reviewed, publicly-available academic paper describing the methodology of that mathematical formula. In basic terms, the methodology relies on two primary facts about the Freenet software: first, the original requestor divides up its requests for pieces of a file among its peers, sending a roughly equal fraction of the requests to each peer; second, if a peer does not have the requested pieces, the peer takes the fraction of requests for pieces of a particular file and divides them up again among its own peers. *See* Figures 1 and 2, *supra*. Because a peer that is merely routing another peer's request would ask its peers for a significantly smaller portion of the pieces of a file than an original requester, it is possible for the recipient of requests to determine whether a request is significantly more likely than not from an original requestor. The academic paper's detailed evaluation finds that a formal mathematical formula based on this reasoning is highly accurate (specifically, it has a high true positive rate and a low false positive rate).⁴ Based upon my training and experience, I believe this to be a reliable method to determine whether it is significantly more probable than not that a given Freenet computer is the original requestor of a file of interest.

23. I am also aware through my training and experience that dozens of searches of digital devices have been conducted by law enforcement officers (either through court-

⁴ That academic paper can be available to the court upon request.

authorization or consent) related to targets whose IP addresses were identified based upon analysis of information from Freenet law enforcement computers, pursuant to which evidence of child pornography possession and/or trafficking was located.

D. Requests Targeted in the Instant Investigation

24. I have reviewed information obtained and logged by law enforcement Freenet computers related to IP address 108.30.166.37 (the “Target IP Address”). Such information shows that a Freenet user with IP address 108.30.166.37 (the “Target Subject”) requested pieces of the child pornography files described below from a law enforcement Freenet computer. With respect to each file – considering the number of requested file pieces, the total number of file pieces required to assemble the file, and the number of peers the user had – the number of requests for file pieces is significantly more than one would expect to see if the user of the Target IP address were merely routing the request of another user. Accordingly – based on my review of those records, my understanding of Freenet, my training and experience, and the fact that the same user requested pieces of multiple child pornography files – I believe that the user of the Target IP address was the original requestor of each of the described files.

25. On November 5, 2019, between 2:31 PM UTC and 3:20 PM UTC, a computer running Freenet software, with the Target IP address, with an average of 51.3 peers, requested from a law enforcement computer 29 out of 1,403 total pieces needed to assemble a file with a SHA1 digital hash value of EISD4IT336ECGP2YFYHDYW273ME4ET3R.⁵ I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet. The file name is

⁵ “SHA1” stands for “secure hash algorithm – 1” and refers to a particular type of cryptographic hash value.

“Boy Girl Suck1.mp4,” and it is a video of a prepubescent girl, approximately nine years old, engaging in oral sex on a prepubescent boy, approximately nine years old.

26. On October 14, 2019, between 4:12 PM UTC and 5:32 PM UTC, a computer running Freenet software, with the Target IP address, with an average of 55.4 peers, requested from a law enforcement computer 42 out of 2,774 total pieces needed to assemble a file with a SHA1 digital hash value of GVYIQ7QYFOJBGYMELSSMOT5W7AMGXR VX. I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet. The file name is “20191001_myhomeismycastle.mkv,” and it is a video of a prepubescent girl, approximately eleven years old, digitally penetrating her vagina.

27. On November 5, 2019, between 2:17 PM UTC and 3:05 PM UTC, a computer running Freenet software, with the Target IP address, with an average of 51.1 peers, requested from a law enforcement computer 25 out of 1,218 total pieces needed to assemble a file with a SHA1 digital hash value of Q6DGK5K725P6K2P4DI7J3WMA6FBSIURM. I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet. The file name is “20191001_myhomeismycastle.mkv,” and it is a video of a prepubescent girl, approximately eleven years old, digitally penetrating her vagina.

28. The fact that a Freenet user requested pieces associated with a particular file on Freenet indicates that the user attempted to download the file’s contents from Freenet. It does not indicate whether or not the user successfully retrieved all of the necessary pieces to successfully download the file.

29. The keys for each of these files were obtained by law enforcement agents at some point between 2011 and the present date either from a Freenet message board or Freesite that contained information related to the sexual exploitation of children, or from a previous

investigation. I am not aware of how, or from where, this particular Freenet user obtained a key in order to attempt to retrieve the files of interest described.

E. Probable Cause Justifying Search of the Subject Premises

30. Open source database searches of the Target IP address identified Verizon Internet Services as the Internet Service Provider. Based on records obtained from Verizon Internet Services by administrative subpoena, the Target IP address was identified as belonging to “221 Husson Ave, Flr 1, Bronx, NY,” which is the first floor of the Subject Premises, and the subscriber as “John Corbett.”

31. A search of records maintained by Con Edison, a public utilities provider to the greater New York City area, shows that an individual by the name of “Patricia Corbett” subscribes to utilities at “221 Husson Ave, Bronx, NY,” which is the Subject Premises.

32. A review of New York City database records showed that an individual named “James Corbett” is receiving public assistance at the Subject Premises.

33. On December 5, 2019, I interviewed James Corbett at the Subject Premises and Corbett provided the following information:

- a. James Corbett resides by himself in the entirety of Subject Premises—that is, he is the sole resident of both the first floor and the second floor.
- b. Patricia Corbett is James Corbett’s grandmother, and she is deceased.
- c. James Corbett’s uncle is the “executor of the house”—that is, of the Subject Premises—and he resides in Carmel, New York.

34. Accordingly, based on the foregoing, I believe that there is probable cause to believe that the Subject Premises contains evidence, fruits, and instrumentalities of the Subject

Offenses, including but not limited to child pornography, computers and mobile devices that were used in committing the Subject Offenses, and evidence of the identity of the Target Subject.

F. Probable Cause Justifying Search of ESI

35. Based on my training and experience, I know that individuals who engage in the Subject Offenses—distribution, receipt, and possession of child pornography—commonly use computers and mobile devices to access websites used for illegal activity, to transmit and download files containing child pornography, to store images and videos containing child pornography, and to communicate with other individuals also engaged in child pornography offenses. As a result, they often store data on their computers and mobile devices related to their illegal activity, which can include email and text message communications, logs of online “chats,” contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts, and contraband materials, including images and videos containing child pornography.

36. Based on my training and experience, I also know that, where computers and mobile devices are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive or mobile device for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.
- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is “deleted” on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in “slack space,” until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or “cache,” which is only overwritten as the “cache” fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user’s operating system, storage capacity, and computer habits.

- In the event that a user changes computers or mobile devices, the user will typically transfer files from the old computer or mobile device to the new one, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

37. In addition to there being probable cause to believe that computer and mobile devices will be found in the Subject Premises that contain evidence of the Subject Offenses, there is also probable cause to believe that these computers and mobile devices constitute instrumentalities of the Subject Offenses in that they were used to receive, transmit, or possess images or videos containing child pornography and they constitute contraband subject to seizure, in that the computers and mobile devices contain contraband child pornography.

38. Based on the foregoing, I respectfully submit there is probable cause to believe that the Target Subject is engaged in child pornography offenses and that evidence of this criminal activity is likely to be found in the Subject Premises and on computers, mobile devices, and electronic media found in the Subject Premises.

III. Procedures for Searching ESI

A. Execution of Warrant for ESI

39. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled

environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of ESI

40. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

41. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and

- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation⁶; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

42. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

43. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

⁶ Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

IV. Conclusion and Ancillary Provisions

44. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

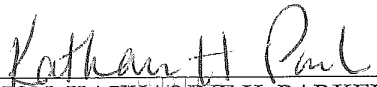
2017.08.02

45. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.



THOMAS A. THOMPSON
Special Agent
Federal Bureau of Investigation

Sworn to before me on
January 17, 2020



HON. KATHARINE H. PARKER
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

The address of the Subject Premises is 221 Husson Avenue, Bronx, New York 10473. The Subject Premises is a two-story residence with white and green siding. A metal fence is in front of the residence. There is a mailbox in front of the residence with the numbers “221,” in gold numbering, on the front of the mailbox. There are two entrances to the Subject Premises, one on each floor. The first-floor entrance to the Subject Premises is on the left side of the front of the residence. The second-floor entrance to the Subject Premises is on the right side of the front of the residence. To the right of the second-floor entrance are the numbers “221” in black numbering. Below is a photograph of the Subject Premises:



II. Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises include the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) and (a)(5) that is, distribution, receipt, and possession of child pornography (the “Subject Offenses”) described as follows:

2017.08.02

USAO_000024

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
2. Any and all computers and mobile devices and any storage devices used to store electronic data, including hard drives, thumb drives, and CDs.
3. Evidence concerning the identity or location of, and communications with, co-conspirators in the Subject Offenses.
4. Any and all books, manuals, guides, or other documents containing information about the operation and ownership of the seized or copied mobile and computer devices or storage media, including, but not limited to, computer, cellular telephone, and software user manuals.
5. Any and all computer software, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs.
6. Any and all video or photograph storage devices, video or photography equipment, or other equipment that aids in the production of child pornography, including, but not limited to, VCRs, DVDs, and videotapes, and their components and accessories, including, but not limited to, wires and cords.
7. Any and all handwritten or typed notes containing computer-related information, including, but not limited to, websites, e-mail addresses, and screen names used to obtain or possess child pornography, minors engaged in sexually explicit conduct, or demonstrating a sexual interest in children.
8. Any and all records and materials, in any format or media (including, but not limited to, e-mail, instant message chat logs, electronic messages, other digital data files, web cache information videos, photographs, photographic negatives, envelopes, letters, or papers) relating to the possession, receipt, shipment, or distribution of child pornography, visual depictions of minors engaged in sexually explicit conduct, or demonstrating a sexual interest in children.
9. Any and all images, Internet histories, Internet site bookmarks, search requests, temporary Internet files, cookies, newsgroups, postings to newsgroups, folder structures and names, and file names stored on seized or copied mobile and computer devices or storage media relating to child pornography, minors engaged in sexually explicit conduct, or demonstrating a sexual interest in children.
10. Any and all information containing evidence of affiliations, memberships, buddy lists, profiles, chat sessions, chat services, billboards, newsgroups, and websites pertaining to child pornography, minors engaged in sexually explicit conduct, or demonstrating a sexual interest in children.
11. Any and all records of communication between individuals concerning the topic of child pornography, having sex with children, the existence of sites on the Internet that contain child pornography or that cater to people with an interest in child pornography, or membership in

online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to their members and constituents.

12. Any and all evidence of any online storage, e-mail, or other remote computer storage subscription, including, but not limited to, unique software relating to such subscription, storage, or email, user logs, archived data that shows connection to such service, or user login and password for such service

13. Any and all data, information, or images evidencing or revealing the unauthorized use of seized or copied mobile and computer devices or storage media by a person other than an owner or authorized user, through the use of viruses, Trojan horses, or other malicious software or infiltration methods.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners, as well as routers, modems, and network equipment used to connect to the Internet. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections II.A and II.B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

See Attachment A

Case No.

20 MAG 00669

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment A

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. §§ 2252A(a)(2) and (a)(5)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before January 31, 2020

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

☐ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court.

USMJ Initials

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

1/17/2020
2:23 p.m.Katharine H. Parker
Judge's signatureCity and state: New York, NY

Hon. Katharine H. Parker, USMJ

Printed name and title

USAO_000028

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.</p>		
Date: _____	<div style="text-align: center;"> <div style="border-bottom: 1px solid black; width: 100%;"></div> <i>Executing officer's signature</i> </div> <div style="text-align: center; margin-top: 10px;"> <div style="border-bottom: 1px solid black; width: 100%;"></div> <i>Printed name and title</i> </div>	

ATTACHMENT A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

The address of the Subject Premises is 221 Husson Avenue, Bronx, New York 10473. The Subject Premises is a two-story residence with white and green siding. A metal fence is in front of the residence. There is a mailbox in front of the residence with the numbers “221,” in gold numbering, on the front of the mailbox. There are two entrances to the Subject Premises, one on each floor. The first-floor entrance to the Subject Premises is on the left side of the front of the residence. The second-floor entrance to the Subject Premises is on the right side of the front of the residence. To the right of the second-floor entrance are the numbers “221” in black numbering. Below is a photograph of the Subject Premises:



II. Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises include the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) and (a)(5) that is, distribution, receipt, and possession of child pornography (the “Subject Offenses”) described as follows:

2017.08.02

USAO_000030

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
2. Any and all computers and mobile devices and any storage devices used to store electronic data, including hard drives, thumb drives, and CDs.
3. Evidence concerning the identity or location of, and communications with, co-conspirators in the Subject Offenses.
4. Any and all books, manuals, guides, or other documents containing information about the operation and ownership of the seized or copied mobile and computer devices or storage media, including, but not limited to, computer, cellular telephone, and software user manuals.
5. Any and all computer software, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs.
6. Any and all video or photograph storage devices, video or photography equipment, or other equipment that aids in the production of child pornography, including, but not limited to, VCRs, DVDs, and videotapes, and their components and accessories, including, but not limited to, wires and cords.
7. Any and all handwritten or typed notes containing computer-related information, including, but not limited to, websites, e-mail addresses, and screen names used to obtain or possess child pornography, minors engaged in sexually explicit conduct, or demonstrating a sexual interest in children.
8. Any and all records and materials, in any format or media (including, but not limited to, e-mail, instant message chat logs, electronic messages, other digital data files, web cache information videos, photographs, photographic negatives, envelopes, letters, or papers) relating to the possession, receipt, shipment, or distribution of child pornography, visual depictions of minors engaged in sexually explicit conduct, or demonstrating a sexual interest in children.
9. Any and all images, Internet histories, Internet site bookmarks, search requests, temporary Internet files, cookies, newsgroups, postings to newsgroups, folder structures and names, and file names stored on seized or copied mobile and computer devices or storage media relating to child pornography, minors engaged in sexually explicit conduct, or demonstrating a sexual interest in children.
10. Any and all information containing evidence of affiliations, memberships, buddy lists, profiles, chat sessions, chat services, billboards, newsgroups, and websites pertaining to child pornography, minors engaged in sexually explicit conduct, or demonstrating a sexual interest in children.
11. Any and all records of communication between individuals concerning the topic of child pornography, having sex with children, the existence of sites on the Internet that contain child pornography or that cater to people with an interest in child pornography, or membership in

online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to their members and constituents.

12. Any and all evidence of any online storage, e-mail, or other remote computer storage subscription, including, but not limited to, unique software relating to such subscription, storage, or email, user logs, archived data that shows connection to such service, or user login and password for such service

13. Any and all data, information, or images evidencing or revealing the unauthorized use of seized or copied mobile and computer devices or storage media by a person other than an owner or authorized user, through the use of viruses, Trojan horses, or other malicious software or infiltration methods.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners, as well as routers, modems, and network equipment used to connect to the Internet. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections II.A and II.B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.